Код Безопасности

Программно-аппаратный комплекс
квалифицированной электронной подписи

"Jinn". Версия 1.0

Руководство администратора

RU.88338853.501430.008 91

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение

Данное руководство предназначено для администраторов изделия "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn". Версия 1.0" RU.88338853.501430.008 (далее — ПАК "Jinn", изделие, комплекс). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации ПАК "Jinn".

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Общие сведения

В корпоративных, территориально распределенных информационных системах могут циркулировать электронные документы, требующие заверения электронной подписью. Существует и признается актуальной атака "человек посередине". Этим человеком может быть физическое лицо, непосредственно взаимодействующее с компьютером ответственного за работу с документом лица, или удаленный злоумышленник, который действует посредством программной атаки (всевозможные вирусы, трояны, черви, руткиты и т. д.) на компьютер ответственного лица из глобальной или локальной сети. Если с первым типом злоумышленника (физическое лицо) можно бороться только организационными мерами, то со вторым необходимо бороться программными или программно-аппаратными средствами. Для защиты именно от второго типа злоумышленника предлагается решение ПАК "Jinn".

Назначение и основные функции

ПАК "Jinn" предназначен для формирования электронной подписи (ЭП) электронного документа, расположенного в ОЗУ компьютера в виде XML-документа, текстового или бинарного файла. Формирование ЭП осуществляется в соответствии с положениями ст. 12 Федерального закона РФ "Об электронной подписи" от 06.04.11 № 63-ФЗ.

ПАК "Jinn" реализует следующие основные функции:

- визуализация электронного документа при отображении подписываемого или проверяемого электронного документа;
- формирование электронной подписи в соответствии с ГОСТ Р 34.10–2001, ГОСТ Р 34.11–94, ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012;
- генерация ключей электронной подписи и формирование запросов на создание сертификатов.

Для проверки правильности работы алгоритма выработки ЭП в комплексе реализована вспомогательная функция контрольного тестирования. Данная функция не используется в качестве целевой функции проверки ЭП.

ПАК "Jinn" можно эксплуатировать совместно со следующими программными продуктами (для файлов с расширениями .txt, .odt, .xml, .pdf) без проведения тематических исследований и/или оценки влияния:

- Adobe Acrobat Reader (от версии 11.0 и выше);
- MS Word 2007, Word 2010, Word 2013.

Назначение электронной подписи

Электронная подпись документа представляет собой данные в электронной форме, присоединяемые к подписываемому электронному документу. Она получается в результате криптографического преобразования информации с использованием ключа подписи.

Электронная подпись позволяет определить лицо, подписавшее электронный документ, а также установить наличие искажений информации в документе. Использование ЭП повышает уровень защищенности документооборота корпоративных информационных систем.

Правовые условия применения ЭП в электронных документах определяются положениями Федерального закона РФ "Об электронной подписи" от 06.04.11 №63-ФЗ. Согласно закону в защищенном документообороте могут использоваться три вида ЭП: простая, неквалифицированная и квалифицированная.

Алгоритмы и процедуры создания ЭП задаются государственными стандартами: формирование и проверка ЭП — ГОСТ Р 34.10–2012, ГОСТ Р 34.10–2001, вычисление хэш-функции — ГОСТ Р 34.11–2012, ГОСТ Р 34.11–94.

Назначение ключевых носителей

Персональный ключевой носитель, выдаваемый пользователю администратором, предназначен для хранения ключевой информации — ключа подписи и сертификата ключа. При подписании документа пользователь предъявляет ключевой носитель, ключевая информация считывается с носителя и с ее помощью создается ЭП пользователя.

Ключ подписи хранится в памяти ключевого носителя в криптографическом контейнере. Криптографический контейнер представляет собой специальным образом организованную папку, содержащую файлы с ключевым материалом. Для предотвращения несанкционированного использования ключа подписи посторонними лицами криптографический контейнер защищают паролем. Ключевой носитель может содержать несколько контейнеров с различными ключами.

Ключ подписи должен однозначно соответствовать сертификату ключа. Для создания ЭП в ПАК "Jinn" предусмотрены два варианта хранения сертификата: на ключевом носителе и в личном хранилище сертификатов Windows.

В качестве ключевых носителей в комплексе могут использоваться аппаратные носители двух типов: USB-флеш-накопители, USB-ключи (Рутокен, eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash) и смарт-карты (eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ).

Для создания ЭП в доверенной среде пользователю комплекса помимо ключевых носителей потребуется идентификатор для входа в ПАК "Соболь" (iButton/USB-ключ (eToken PRO, eToken PRO (Java), iKey 2032, Рутокен, Рутокен RF)/смарт-карта eToken PRO) или загрузочный USB-флеш-накопитель.

Принципы функционирования

Доверенная среда

Доверенная визуализация и подпись документа осуществляются в доверенной среде. Доверенная среда (ДС) — это выполняющаяся на компьютере клиента микропрограмма, которая функционирует одновременно с клиентской операционной системой (ОС). ДС — это не операционная система, а микрокод, который загружается в кеш процессора и регистры процессора при старте компьютера с USB-флеш-накопителя. Микрокод работает только "внутри" процессора, т. е. он не отображается в оперативную память и недоступен для изменения извне, т.е. из других процессоров.

Компоненты комплекса

В состав ПАК "Jinn" входит программный компонент "Jinn-Client", предназначенный для формирования ЭП документа, содержащий программное обеспечение автоматизированного рабочего места генерации ключей (АРМ ГК), предназначенного для генерации ключей ЭП формата PKCS#15 и формирования запросов на создание сертификатов формата PKCS#10.

Для проверки правильности работы алгоритма выработки ЭП в "Jinn-Client" реализована функция контрольного тестирования. Данная функция не может быть использована в качестве целевой функции проверки ЭП.

Программное обеспечение "Jinn-Client" состоит из двух компонентов:

- "Jinn-TE" — представляет собой специализированное программное обеспечение доверенной среды (СПО ДС), которое записывается в память USB-флеш-накопителя (для исполнений комплекса 1–6) или ПАК "Соболь" (для исполнений комплекса 3, 4) и загружается в процессор компьютера во время

включения или перезагрузки компьютера до старта загрузки клиентской операционной системы (ОС) на рабочих местах пользователей;

- "Jinn-Service" — представляет собой специализированное программное обеспечение, функционирующее в ОС семейства Windows (СПО ОС). "Jinn-Service" состоит из специализированного программного компонента интерфейса обмена с СПО ДС и специализированного программного компонента эмуляции ДС в ОС, реализующего функционал СПО ДС "Jinn-TE" при отсутствии запущенного СПО ДС "Jinn-TE".

СПО ДС "Jinn-TE" обеспечивает:

- запуск микропрограммы ДС до старта клиентской ОС;
- реализацию функции электронной подписи (ГОСТ Р 34.10–2001 или ГОСТ Р 34.10–2012), не использующей механизмы клиентской ОС;
- отображение на экране компьютера подписываемого документа без использования механизмов клиентской ОС;
- работу с аутентифицирующей информацией без использования механизмов клиентской ОС;
- работу с ключом электронной подписи без использования механизмов клиентской ОС.

СПО ОС "Jinn-Service" обеспечивает:

- интерфейс для обращения к функционалу СПО ДС "Jinn-TE" из прикладного программного обеспечения, функционирующего в ОС;
- эмуляцию СПО ДС "Jinn-TE" в ОС при функционировании в режиме неактивного СПО ДС "Jinn-TE".

В исполнениях комплекса 3 и 4 для обеспечения запуска ДС с помощью сертифицированного ФСБ России ПАК "Соболь" осуществляется модификация кода расширения BIOS ПАК "Соболь". Модификация не вносит изменения в специальные свойства ПАК "Соболь". Модификация заключается в реализации в BIOS ПАК "Соболь" дополнительной процедуры старта СПО ДС "Jinn-TE". Данная процедура проводится после завершения штатных процедур ПАК "Соболь" и перед передачей управления загрузочному сектору основного жесткого диска. После запуска СПО ДС ПАК "Соболь" штатно передает управление загрузочному сектору основного жесткого диска для загрузки клиентской ОС.

АРМ ГК обеспечивает:

- генерацию ключевой пары и формирование криптографического контейнера на основе стандарта PKCS#15;
- формирование запросов по стандарту PKCS#10 на выдачу сертификата в удостоверяющем центре;
- формирование загрузочного USB-флеш-накопителя с СПО ДС "Jinn-TE";
- импорт файлов сертификата и криптографического контейнера формата PKCS#15 на съемный носитель.

АРМ ГК функционирует совместно с ПАК "Соболь" (для исполнений комплекса 3, 4, 7, 8).

Варианты исполнения

ПАК "Jinn" выпускается в следующих вариантах исполнения.

№ исп.	Наименование исполнения	Применение ПАК "Соболь"	Формирование и проверка ЭП	Вычисление хэш-функции
1	Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Client". Версия 1.0	Нет	ГОСТ Р 34.10–2001	ГОСТ Р 34.11–94

№ исп.	Наименование исполнения	Применение ПАК "Соболь"	Формирование и проверка ЭП	Вычисление хэш-функции
2	Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Client". Версия 1.0	Нет	ГОСТ Р 34.10–2012	ГОСТ Р 34.11–2012
3	Программа доверенной визуализации и подписи "Jinn-Client". Версия 1.0	Да	ГОСТ Р 34.10–2001	ГОСТ Р 34.11–94
4	Программа доверенной визуализации и подписи "Jinn-Client". Версия 1.0	Да	ГОСТ Р 34.10–2012	ГОСТ Р 34.11–2012
5	Программа доверенной визуализации и подписи "Jinn-Client". Версия 1.0	Нет	ГОСТ Р 34.10–2001	ГОСТ Р 34.11–94
6	Программа доверенной визуализации и подписи "Jinn-Client". Версия 1.0	Нет	ГОСТ Р 34.10–2012	ГОСТ Р 34.11–2012
7	Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Admin". Версия 1.0	Да	ГОСТ Р 34.10–2001	ГОСТ Р 34.11–94
8	Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Admin". Версия 1.0	Да	ГОСТ Р 34.10–2012	ГОСТ Р 34.11–2012
9	Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Admin". Версия 1.0	Нет	ГОСТ Р 34.10–2012	ГОСТ Р 34.11–2012

Исполнения 5, 6, 9 ПАК "Jinn" соответствуют требованиям ФСБ России к криптографическим средствам класса КС1, исполнения 1–4, 7, 8 – класса КС2.

Системные требования

Компьютеры, на которых предполагается использовать ПАК "Jinn", должны соответствовать следующим аппаратным и программным требованиям:

Операционная система	MS Windows 10, 8.1 x86/x64, 8 x86/x64, 7 SP1 x86/x64, Vista SP2 x86/x64 (кроме всех выпусков Starter); MS Windows XP Professional SP3 x86/x64; MS Windows 2008 Server SP2 x86/x64, 2008 Server R2 SP1 x64, 2003 Server R2 SP2 x86/x64, 2003 Server SP2 x86/x64
Процессор при использовании режима эмуляции доверенной среды (ДС) в ОС (исполнения 7, 8, 9 и 3–6 в режиме эмуляции ДС в ОС)	В соответствии с требованиями ОС, установленной на компьютер
Процессор при использовании режима ДС (исполнения 1,2 и 3–6 в режиме ДС)	Многоядерный (2 и более) процессор Intel должен поддерживать технологии Intel-VT (VT-x) и EPT. Многоядерный (2 и более) процессор AMD должен поддерживать технологию AMD-V
Оперативная память	В соответствии с требованиями ОС, установленной на компьютер
Жесткий диск (свободное место)	50 МБ
Привод	Привод DVD/CD-ROM

Интерфейсы	2 x USB 2.0; 1 x PCI-E — для исполнений 3, 4, 7, 8, 9
Дополнительное ПО	ПАК "Соболь" — для исполнений 3, 4, 7, 8

- Доверенная среда несовместима с энергосберегающим режимом "Гибернация" ОС Windows.
- На компьютерах с материнскими платами производителя ASUS, использующих некоторые старые версии BIOS, возможны проблемы с загрузкой доверенной среды с USB-флеш-накопителей, подключенных к порту USB 3.0. Для устранения таких проблем рекомендуется обновить BIOS до последней версии. Также можно использовать имеющийся в BIOS режим загрузки компьютера по нажатии клавиши F8 или в настройках загрузки BIOS указывать конкретное устройство, с которого выполняется загрузка.

Порядок распространения и тиражирования

Установочные модули ПО ПАК "Jinn" и комплект эксплуатационной документации к нему могут поставляться пользователю Уполномоченной организацией двумя способами:

- на носителе (CD-, DVD-диски);
- посредством загрузки через Интернет.

Для получения возможности загрузки установочных модулей ПО ПАК "Jinn" и комплекта эксплуатационной документации пользователь направляет свои учетные данные Уполномоченной организации. Учетные данные могут быть направлены посредством заполнения специализированной регистрационной формы на сайте Уполномоченной организации.

После получения Уполномоченной организацией учетных данных пользователю предоставляется доступ на страницу загрузки установочных модулей ПО ПАК "Jinn" и комплекта эксплуатационной документации (далее — страница загрузки). При загрузке пользователем установочных модулей ПО ПАК "Jinn" и комплекта эксплуатационной документации Уполномоченной организацией присваивается учетный номер, идентифицирующий экземпляр ПО ПАК "Jinn", предоставленный пользователю.

Установка ПО ПАК "Jinn" на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей ПО ПАК "Jinn" и эксплуатационной документации.

На странице загрузки вместе с дистрибутивом и эксплуатационной документацией размещается файл integrity_msi.xml, содержащий значения электронной подписи, рассчитанные для всех файлов, составляющих дистрибутив. Для проверки целостности дистрибутива необходимо использовать утилиту ICheck_msi.exe, полученную доверенным образом и содержащую соответствующий ключ проверки. Ключ проверки ЭП, а также информация о нем (дата создания, алгоритм хэш-функции, идентификатор алгоритма подписи) записываются в исходный код утилиты на этапе сборки.

Средство контроля целостности Icheck_msi.exe первоначально должно быть получено пользователем на физическом носителе в офисе компании "Код Безопасности" либо у официального дилера. Такая утилита считается полученной доверенным образом. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом, например, скачанная с сайта www.securitycode.ru, при условии, что она была проверена другим экземпляром утилиты, полученным ранее доверенным образом, и проверка прошла успешно.

Глава 2
Установка и настройка

Установка ПАК "Соболь"

Если в комплект поставки ПАК "Jinn" входит ПАК "Соболь", то перед установкой ПО ПАК "Jinn" необходимо выполнить установку и настройку ПАК "Соболь" в соответствии с документом "Программно- аппаратный комплекс "Соболь". Руководство администратора".

Если загрузка доверенной среды выполняется из памяти ПАК "Соболь" (исполнения ПАК "Jinn" 3 и 4), при его инициализации необходимо выполнить настройку параметров доверенной среды. В этом случае после диалога настройки общих параметров ПАК "Соболь" на экране появится диалог "Доверенная среда (Jinn)". Описание параметров диалога приводится в следующей таблице.

Запускать ДС
Параметр управляет загрузкой доверенной среды при старте компьютера: "Да" — загрузка доверенной среды выполняется, "Нет" — загрузка не выполняется.
Режим работы ДС
Параметр управляет режимами работы доверенной среды: "Мягкий", "Жесткий". Работа в жестком режиме обеспечивает более совершенную защиту документа при его визуализации. Но этот режим применим не для всех видеокарт и может вызвать нарушения в работе доверенной среды. Рекомендуется использовать мягкий режим. Если же жесткий режим используется в системе, в которой не определен драйвер видеокарты, при визуализации на экране может появиться сообщение "Невозможно получить настройки видеоадаптера". В этом случае необходимо корректно установить драйвер данной видеокарты.
Всегда визуализировать документ
Параметр определяет, разрешить (значение "Нет") или запретить (значение "Да") подписывать документ без его визуализации. В случае установки запрета подписание документов без их предварительной визуализации средствами ПАК "Jinn" невозможно. Подписывать можно будет только текстовые и XML-документы, бинарные документы подписать будет нельзя.

Совет. После инициализации ПАК "Соболь" настройку параметров доверенной среды можно выполнить, используя меню администратора. Войдите с правами администратора в ПАК "Соболь", выберите пункт меню "Параметры ДС (Jinn)" и настройте указанные выше параметры.

Установка программного обеспечения

Пользователь, устанавливающий ПО ПАК "Jinn", должен обладать правами администратора компьютера — входить в локальную группу администраторов.

Доверенная среда несовместима с энергосберегающим режимом "Гибернация" ОС Windows. Перед установкой ПАК "Jinn" необходимо отключить этот режим и обеспечить средствами администрирования ОС Windows запрет на использование этого режима пользователями.

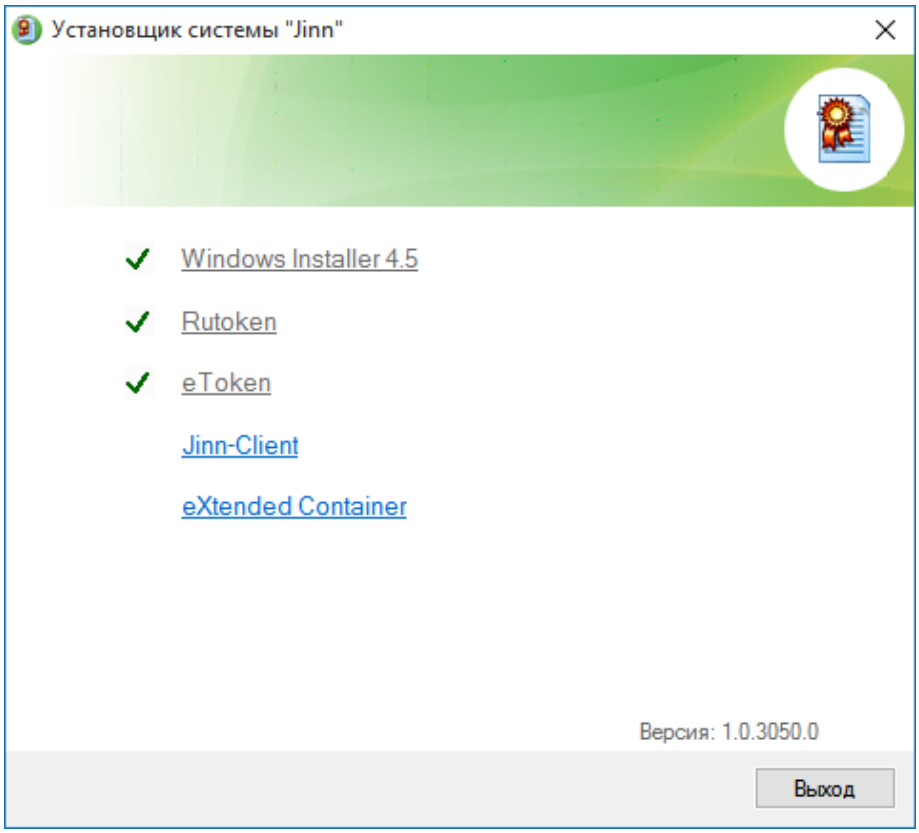
Для установки ПО используется интегральная программа установки, которая при запуске определяет перечень необходимых для установки и уже установленных компонентов ПАК "Jinn" и дополнительного ПО.

Для запуска интегральной программы установки:

1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск с ПО ПАК "Jinn" в устройство чтения компакт-дисков и запустите на исполнение файл:
   - CD\setup.exe — если не требуется использовать в составе решения ПАК "Соболь" (исполнения 1, 2, 5, 6, 9);

- CD_Sable\setup.exe — если требуется использовать в составе решения ПАК "Соболь" (исполнения 3, 4, 7, 8).

На экране появится диалог интегральной программы установки.



Диалог содержит список гиперссылок с названиями ПО, необходимого для работы. Если слева от названия ПО содержится отметка — значит, данное ПО уже установлено на компьютере и его установка не требуется.

Примечание. Если гиперссылка "Jinn-Client" содержит слово "обновление" — значит, на компьютере установлен этот компонент предыдущей версии. Используйте данную гиперссылку для запуска процедуры обновления компонента, которая аналогична процедуре установки.

Установка дополнительного ПО

Если на компьютере отсутствует нужная версия Windows Installer или предполагается использовать ПАК "Jinn" с персональными ключевыми носителями, необходимо выполнить установку дополнительного ПО.

Для установки дополнительного ПО:

1. В диалоге интегральной программы установки (см. стр.**11**) активируйте гиперссылку:
   - "Windows Installer 4.5" — если на компьютере отсутствует нужная версия Windows Installer;
   - "Rutoken" — если предполагается использовать персональные ключевые носители Рутокен;
   - "eToken" — если предполагается использовать персональные ключевые носители eToken PRO и eToken PRO (Java).

   Примечание. Если слева от гиперссылки имеется отметка, данный продукт уже установлен.

   На экране появится диалог программы установки.
2. Выполните действия, предлагаемые программой установки.

По завершении установки активная гиперссылка будет заблокирована и слева от нее появится отметка, указывающая на то, что данный продукт установлен.

Для работы с персональными ключевыми носителями JaCarta:

1. Поместите установочный диск с ПО ПАК "Jinn" в устройство чтения компакт-дисков, перейдите в папку ..\prerequisites этого диска и запустите один из файлов, в соответствии с установленной версией операционной системы:
   - JaCartaUnifiedClient_2.9.0.1531_win-x64_ru-Ru.msi
   - JaCartaUnifiedClient_2.9.0.1531_win-x86_ru-Ru.msi
2. Выполните действия, предлагаемые программой установки.

Установка ПО "Jinn-Client"

Для установки ПО:

1. В диалоге интегральной программы установки (см. стр. **11**) активируйте гиперссылку "Jinn-Client".

   Программа установки выполнит подготовительные действия, после чего на экране появится стартовый диалог программы.

   Совет. Для управления процессом установки используйте кнопки:
   - "Назад" — для возврата к предыдущему диалогу;
   - "Далее" — для перехода к следующему диалогу;
   - "Отмена" — для прекращения процесса установки. После нажатия этой кнопки подтвердите свое решение в появившемся окне запроса.

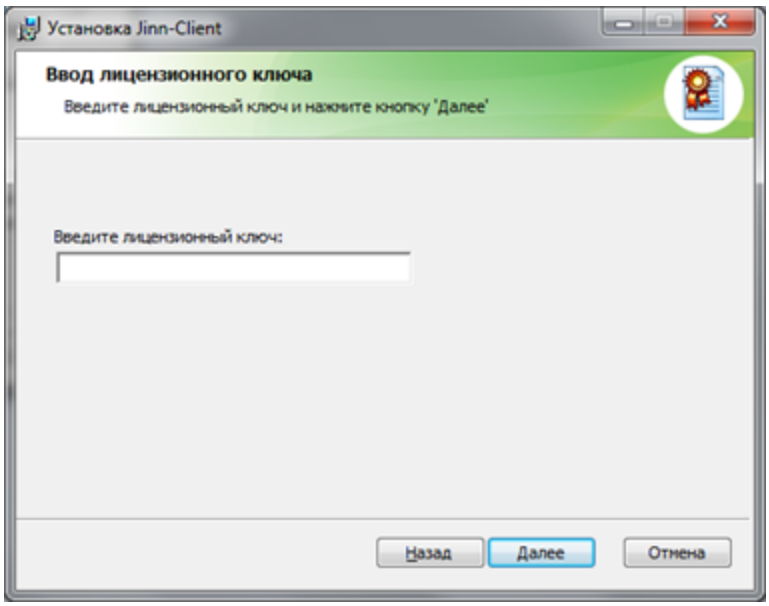
2. Нажмите кнопку "Далее" для продолжения установки.

   На экране появится диалог с лицензионным соглашением на использование программного продукта.

3. Прочтите лицензионное соглашение и, если вы принимаете его условия, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

   Совет. Для вывода текста лицензионного соглашения на печать используйте кнопку "Печать".

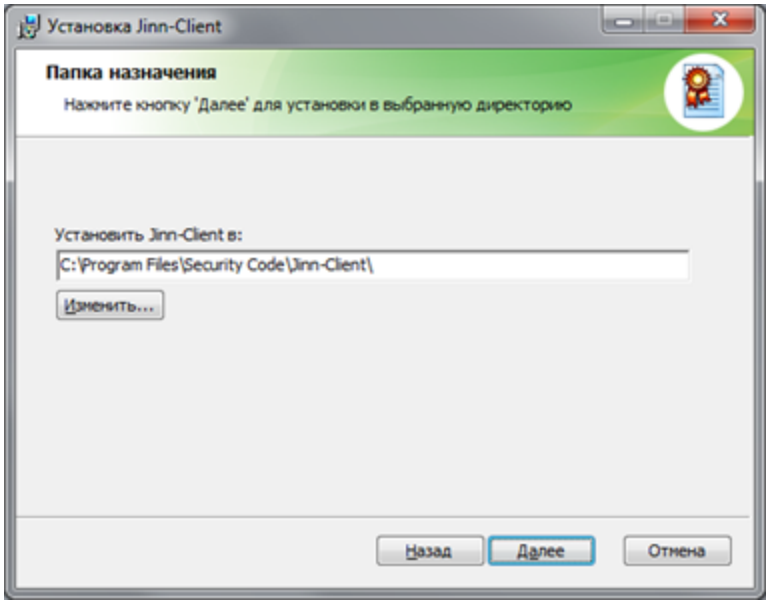
   На экране появится диалог для ввода лицензионного ключа продукта.



4. Введите в текстовом поле диалога лицензионный ключ продукта и нажмите кнопку "Далее".

   Примечание. Без ввода правильного лицензионного ключа установка невозможна.

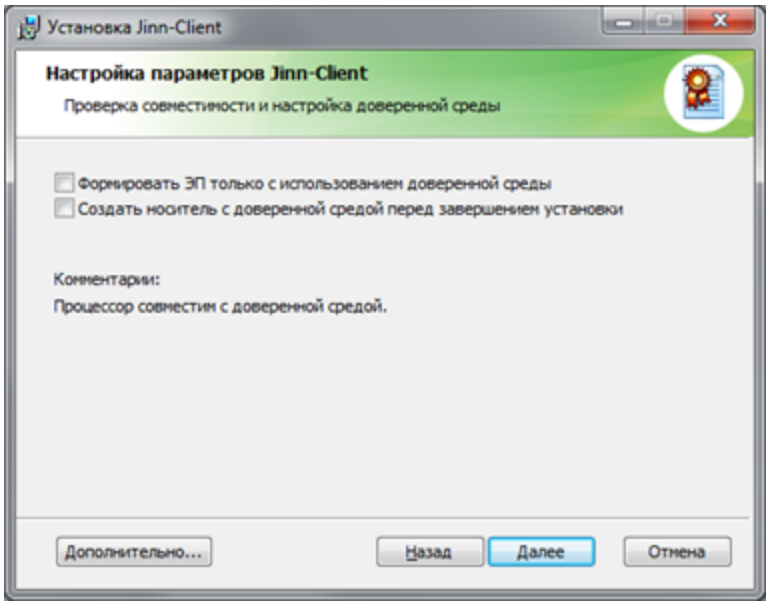
   На экране появится диалог выбора папки для размещения файлов продукта.



5. При необходимости укажите другую папку. Нажмите кнопку "Далее".

Примечание. По умолчанию файлы размещаются на системном диске в папке \Program Files\Security Code\Jinn-Client\. Для выбора другой папки используйте кнопку "Изменить".

На экране появится диалог настройки параметров работы продукта.



Примечание. В поле "Комментарии" приводится результат проверки совместимости процессора компьютера с технологией создания доверенной среды. В зависимости от этого результата некоторые поля диалога могут быть недоступны для управления.

6. Настройте параметры и нажмите кнопку "Далее".

Формировать ЭП только с использованием доверенной среды
Отметьте это поле, если требуется, чтобы все операции с документами выполнялись только в доверенной среде. Если отметка не установлена, работа с документами будет выполняться в стандартной среде ОС. Доверенную среду в этом случае использовать будет нельзя. **Внимание!** Это параметр настраивается только при установке. Для его изменения необходимо будет выполнить повторную установку "Jinn-Client".

Создать носитель с доверенной средой перед завершением установки
Отметьте это поле, чтобы создать USB-флеш-накопитель для загрузки доверенной среды в процессе установки продукта. Нужно учитывать, что при выполнении этой операции USB-флеш-накопитель будет отформатирован и содержащиеся на нем данные будут потеряны. В дальнейшем загрузочный USB-флеш-накопитель можно будет создать с помощью АРМ ГК (см. стр.**17**).
Всегда визуализировать документ
Нажмите кнопку "Дополнительно" и в появившемся диалоге отметьте это поле, если требуется, чтобы перед подписанием любого документа всегда выполнялась его визуализация. В этом режиме подписание документов без их предварительной визуализации средствами ПАК "Jinn" невозможно. Подписывать можно будет только текстовые и XML-документы, бинарные документы подписать будет нельзя. **Внимание!** Этот параметр используется при работе с документами в стандартной среде ОС без применения доверенной среды и настраивается только при установке. Для его изменения необходимо будет выполнить повторную установку "Jinn-Client".

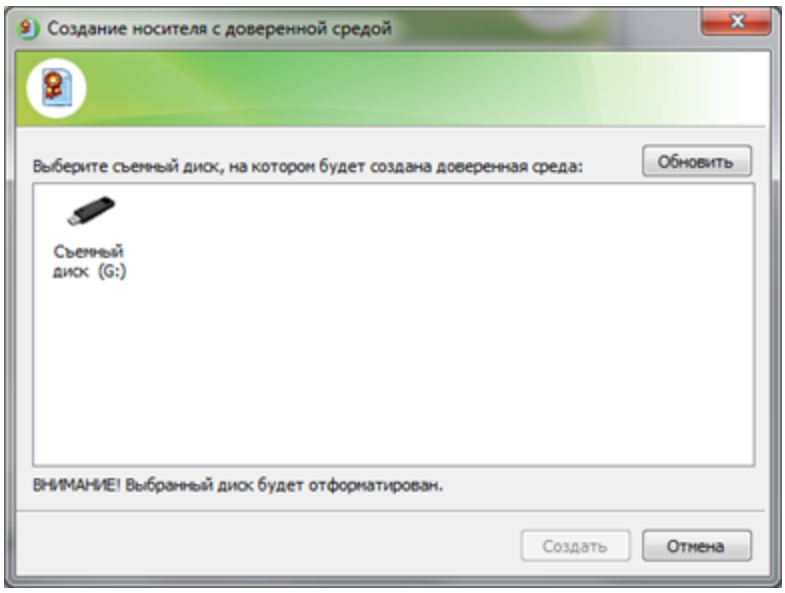
На экране появится диалог с сообщением о готовности к установке.

Совет. Это последний шаг, на котором можно изменить параметры установки. Для возврата к предыдущим шагам используйте кнопку "Назад".

7. Нажмите кнопку "Установить".

   Программа установки приступит к копированию файлов. Ход процесса установки отображается в виде индикатора прогресса.

   Если был включен режим "Создать носитель с доверенной средой перед завершением установки", на экране появится диалог выбора носителя.



Выбранный USB-флеш-накопитель будет отформатирован и содержащиеся на нем данные будут потеряны.

8. Вставьте USB-флеш-накопитель в свободный USB-разъем и нажмите кнопку "Обновить".
9. Выберите появившийся в списке диалога накопитель и нажмите кнопку "Создать".

   Начнется создание загрузочного USB-флеш-накопителя. При успешном завершении этой процедуры на экране появится сообщение об этом.

10. Извлеките USB-флеш-накопитель из USB-разъема и нажмите кнопку "ОК" в окне сообщения.

    На экране появится заключительный диалог программы установки.

11. Нажмите кнопку "Готово".

    На экране появится сообщение о необходимости перезагрузки компьютера.

12. Нажмите кнопку "Да" в окне сообщения.

Начнется перезагрузка компьютера.

В результате установки компонента "Jinn-Client" в меню "Все программы" главного меню Windows добавится подменю "Код Безопасности|Jinn" с командой "Создание доверенной среды".

После установки ПО "Jinn-Client" необходимо выполнить его сопряжение с клиентским программным обеспечением потребителя. См. документ "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn". Версия 1.0. Руководство программиста".

Установка опционального ПО "eXtended Container"

Примечание. Для установки и использования данного ПО необходима соответствующая лицензия на право пользования.

Для установки ПО:

1. В диалоге интегральной программы установки (см. стр. **11**) активируйте гиперссылку "eXtended Container".

Программа установки выполнит подготовительные действия, после чего на экране появится стартовый диалог программы.

Совет. Для управления процессом установки используйте кнопки:
- "Назад" — для возврата к предыдущему диалогу;
- "Далее" — для перехода к следующему диалогу;
- "Отмена" — для прекращения процесса установки. После нажатия этой кнопки подтвердите свое решение в появившемся окне запроса.

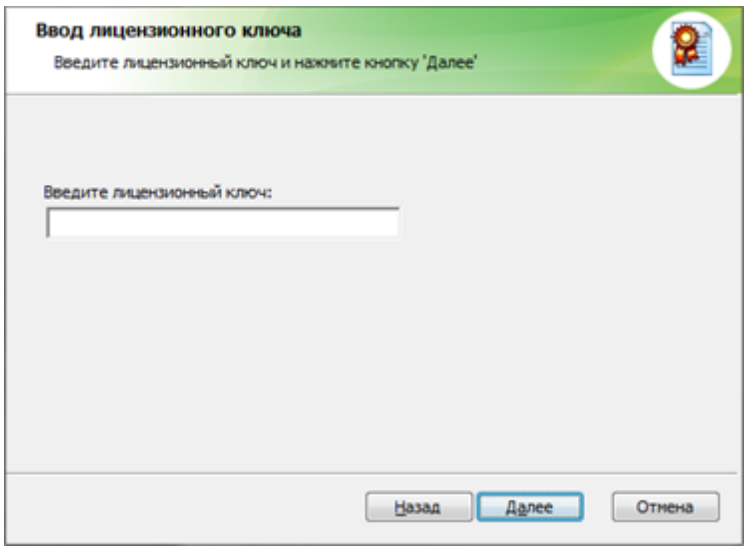
2. Нажмите кнопку "Далее" для продолжения установки.

На экране появится диалог с лицензионным соглашением на использование программного продукта.

3. Прочтите лицензионное соглашение и, если вы принимаете его условия, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

Совет. Для вывода текста лицензионного соглашения на печать используйте кнопку "Печать".

На экране появится диалог для ввода лицензионного ключа продукта.



4. Введите в текстовом поле диалога лицензионный ключ продукта и нажмите кнопку "Далее".

Примечание. Без ввода правильного лицензионного ключа установка невозможна.

На экране появится диалог выбора папки для размещения файлов продукта.

5. При необходимости укажите другую папку. Нажмите кнопку "Далее".

На экране появится диалог с сообщением о готовности к установке.

Совет. Это последний шаг, на котором можно изменить параметры установки. Для возврата к предыдущим шагам используйте кнопку "Назад".

6. Нажмите кнопку "Установить".

   Программа установки приступит к копированию файлов. Ход процесса установки отображается в виде индикатора прогресса. По завершении установки на экране появится заключительный диалог программы установки.

7. Нажмите кнопку "Готово".

Глава 3
Управление комплексом

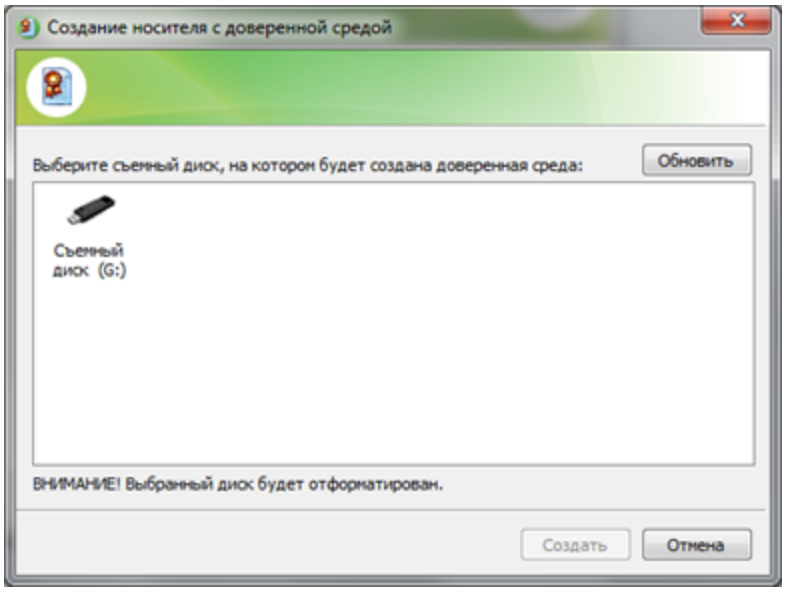
Создание загрузочного носителя в "Jinn-Client"

Для работы с доверенной средой необходимо создать загрузочный USB-флеш-накопитель.

Для создания загрузочного USB-флеш-накопителя:

1. Нажмите кнопку "Пуск" и активируйте в главном меню Windows команду "Все программы|Код Безопасности|Jinn|Создание доверенной среды".

   На экране появится диалог выбора носителя.



Выбранный USB-флеш-накопитель будет отформатирован и содержащиеся на нем данные будут потеряны.

2. Вставьте USB-флеш-накопитель в свободный USB-разъем и нажмите кнопку "Обновить".
3. Выберите появившийся в списке диалога накопитель и нажмите кнопку "Создать".

   Начнется создание загрузочного USB-флеш-накопителя. При успешном завершении этой процедуры на экране появится сообщение об этом.
4. Извлеките USB-флеш-накопитель из USB-разъема и нажмите кнопку "ОК" в окне сообщения.

Работа с АРМ ГК

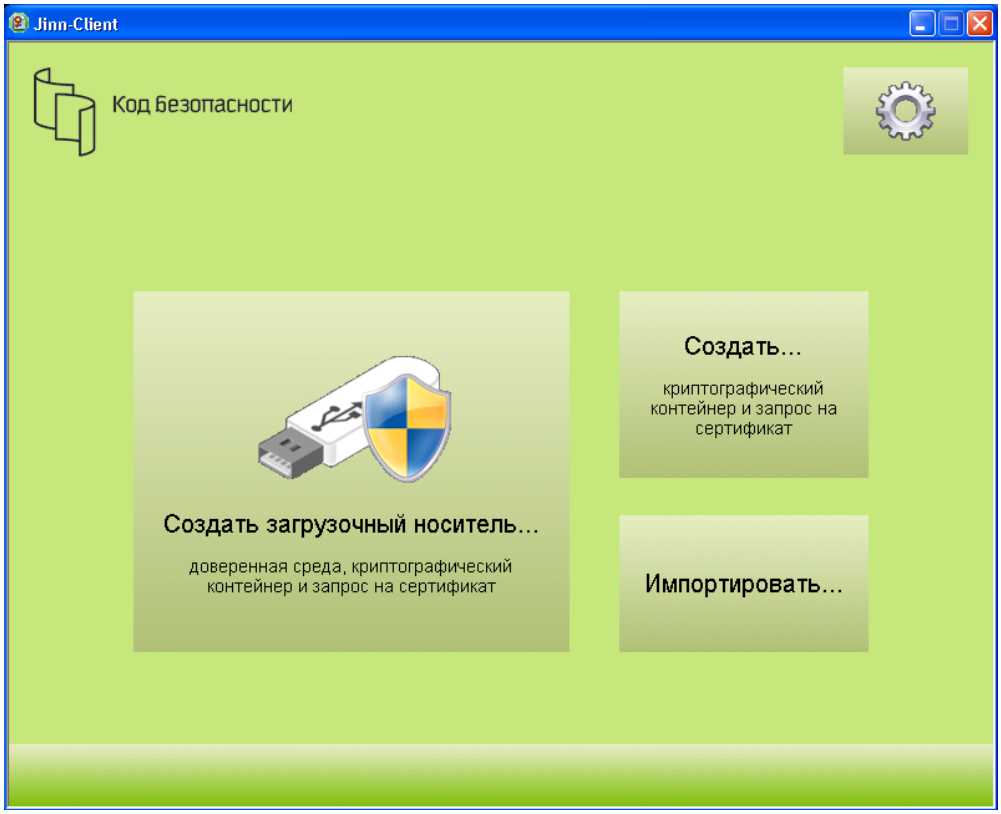
АРМ ГК обеспечивает:

- создание загрузочных USB-флеш-накопителей с доверенной средой;
- формирование запроса на выдачу сертификата в удостоверяющий центр, включая создание криптографического ключа сертификата;
- запись на ключевой носитель сертификата и криптографического контейнера формата PKCS#15.

Для запуска АРМ ГК:

- Нажмите кнопку "Пуск" и активируйте в главном меню Windows команду "Все программы|Код Безопасности|Jinn|Jinn-Client".

На экране появится основное окно программы.



В центральной части окна размещаются три кнопки, обеспечивающие запуск одноименных процедур.

В верхнем правом углу окна находится кнопка, вызывающая служебное меню.

Создание загрузочного USB-флеш-накопителя

Мастер создания загрузочного USB-флеш-накопителя позволяет:

- создать загрузочный USB-флеш-накопитель;
- создать запрос на издание сертификата и соответствующий ему криптографический контейнер и записать их на USB-флеш-накопитель;
- записать на USB-флеш-накопитель имеющиеся сертификат и криптографический контейнер формата PKCS#15.

Для создания загрузочного USB-флеш-накопителя:

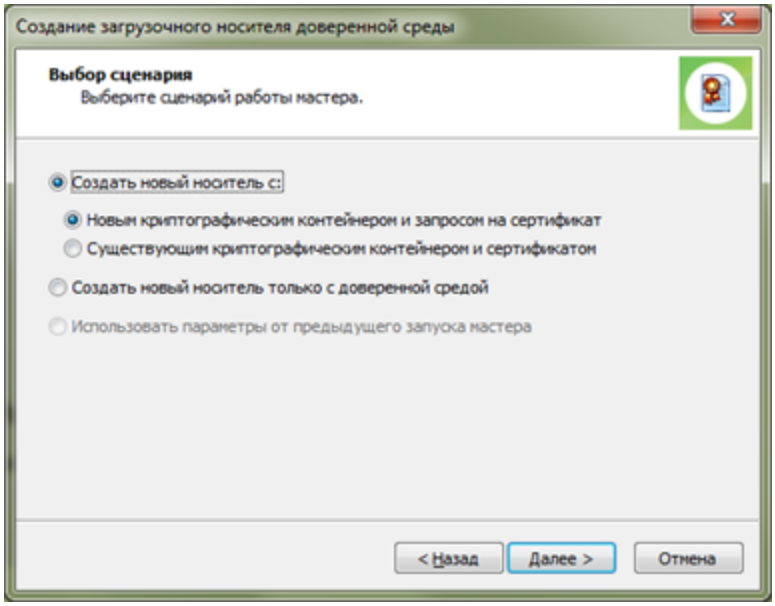
1. В основном окне программы нажмите кнопку "Создать загрузочный носитель...".

   На экране появится стартовый диалог программы-мастера.

   Совет. Если показывать этот диалог больше не требуется, отметьте поле "Не показывать ...".

2. Нажмите кнопку "Далее >".

   На экране появится диалог выбора варианта продолжения процедуры.



3. Выберите вариант продолжения процедуры и нажмите кнопку "Далее >".
   - Выберите вариант "Создать новый носитель с:" и затем вариант "Новым криптографическим контейнером и запросом на сертификат" — чтобы при создании загрузочного USB-флеш-накопителя также создать запрос на издание сертификата пользователя, соответствующий ему криптографический контейнер и записать их на данный USB-флеш-накопитель.

     При выборе этого варианта после нажатия кнопки "Далее >" перейдите к выполнению действия **3** процедуры создания запроса на сертификат (см. стр.**19**).
   - Выберите вариант "Создать новый носитель с:" и затем вариант "Существующим криптографическим контейнером и сертификатом" — чтобы при создании загрузочного USB-флеш-накопителя также записать на него имеющийся сертификат пользователя и соответствующий ему криптографический контейнер формата PKCS#15.

     При выборе этого варианта после нажатия кнопки "Далее >" перейдите к выполнению действия **3** процедуры записи сертификата и криптоконтейнера на носитель (см. стр.**22**).
   - Выберите "Создать новый носитель только с доверенной средой" — будет создан только загрузочный USB-флеш-накопитель.

     При выборе этого варианта после нажатия кнопки "Далее >" перейдите к выполнению действия **2** процедуры создания загрузочного USB-флеш-накопителя (см. стр.**17**).
   - Выберите "Использовать параметры от предыдущего запуска мастера" — будет выполнен вариант процедуры, который использовался при предыдущем запуске мастера в текущем сеансе работы с программой.

Создание запроса на сертификат

Мастер создания криптографического контейнера и запроса на сертификат позволяет создать криптографический контейнер, запрос на издание сертификата пользователя и записать их на съемный носитель.

Для создания запроса:

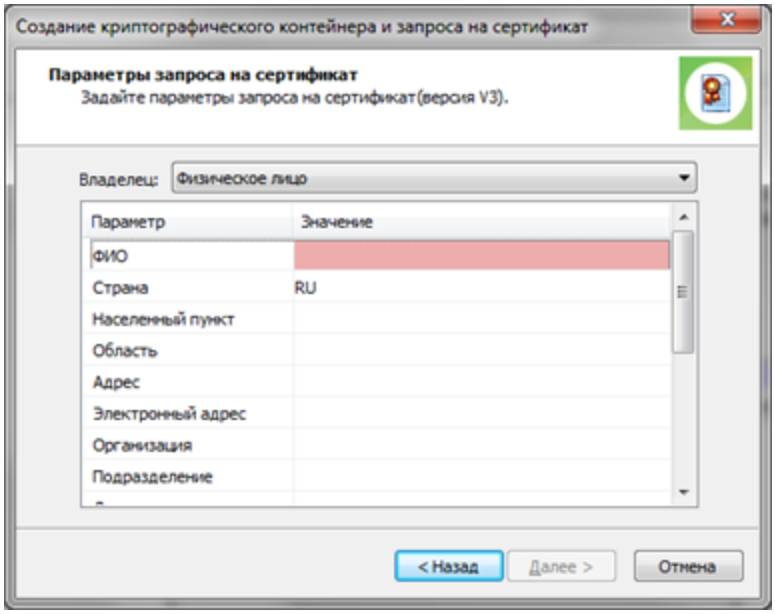
1. В основном окне программы нажмите кнопку "Создать...".

   На экране появится стартовый диалог программы-мастера.

   Совет. Если показывать этот диалог больше не требуется, отметьте поле "Не показывать ...".

2. Нажмите кнопку "Далее >".

   На экране появится диалог для ввода параметров запроса.

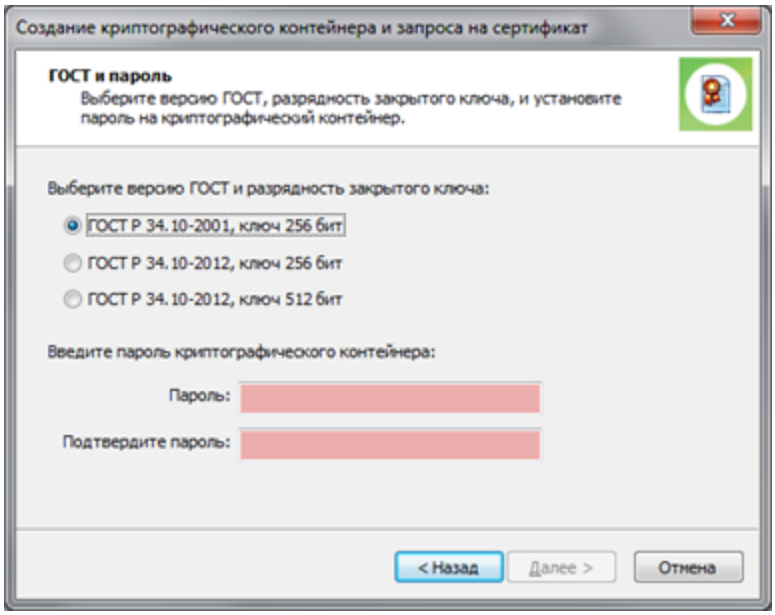


3. Настройте параметры запроса и нажмите кнопку "Далее >".

- В поле "Владелец" выберите из раскрывающегося списка нужное значение.
- В таблице с параметрами укажите нужные параметры владельца сертификата.

> **Совет.** Для ввода значения параметра активируйте щелчком мыши поле в столбце "Значение". Параметры, обязательные для заполнения, отмечены красным цветом.

На экране появится диалог для выбора параметров закрытого ключа и ввода пароля доступа к криптографическому контейнеру.

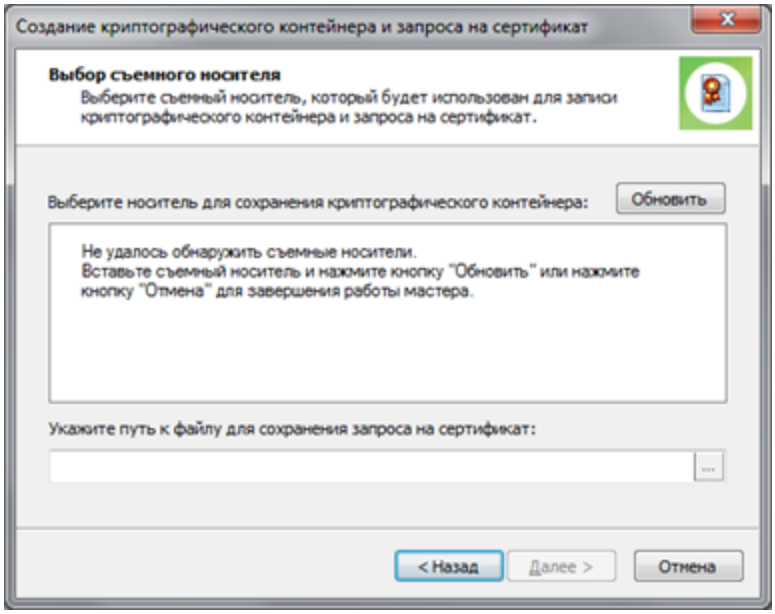


4. Настройте параметры диалога и нажмите кнопку "Далее >".

- Выберите версию ГОСТ и разрядность, которые будут использоваться при создании закрытого ключа сертификата.
- Дважды введите пароль, с помощью которого будет защищен доступ к закрытому ключу, хранящемуся в создаваемом контейнере.

> **Совет.** Запомните или запишите пароль. Этот пароль необходимо сообщить пользователю. Не зная пароля, он не сможет использовать изданный сертификат.

На экране появится диалог выбора носителя.



5. В нижнем поле диалога укажите полный путь к файлу, в котором будет сохранен запрос на издание сертификата пользователя.

   Совет. Для выбора места размещения файла в диалоговом режиме нажмите кнопку "..." в правой части поля.

6. Вставьте USB-флеш-накопитель в свободный USB-разъем и нажмите кнопку "Обновить".
7. Выберите появившийся в списке диалога накопитель и нажмите кнопку "Далее >".

   На экране появится диалог выбора места хранения резервной копии криптографического контейнера.
8. В поле диалога укажите полный путь к файлу резервной копии создаваемого криптографического контейнера и нажмите кнопку "Далее >".

   Примечание. Если резервную копию криптографического контейнера создавать не требуется, оставьте поле пустым и нажмите кнопку "Далее >".

   Далее для создания запроса потребуется генерация набора случайных чисел. Если используется датчик ПАК "Соболь", то набор энтропии выполняется автоматически и на экране не отображается. Перейдите к п. 8.

   В противном случае на экране появится окно, предназначенное для накопления энтропии.
9. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.
10. В указанной папке будет сформирован файл запроса сертификата, а на носителе будет записан ключевой контейнер. Дождитесь сообщения о завершении процесса создания запроса и закройте его.
11. Извлеките носитель из USB-разъема и нажмите кнопку "Готово".

Запись сертификата и криптографического контейнера на носитель

Мастер импорта криптографического контейнера и сертификата позволяет записать имеющиеся файлы сертификата и криптографического контейнера в формате PKCS#15 на съемный носитель.

Примечание. Если используемый съемный носитель содержит файлы, имена которых совпадают с именами записываемых файлов:

- файлы на USB-флеш-накопителе будут автоматически переименованы и сохранены;
- файлы на eToken, Рутокен будут перезаписаны с выводом запроса на выполнение операции.

Для записи файлов на носитель:

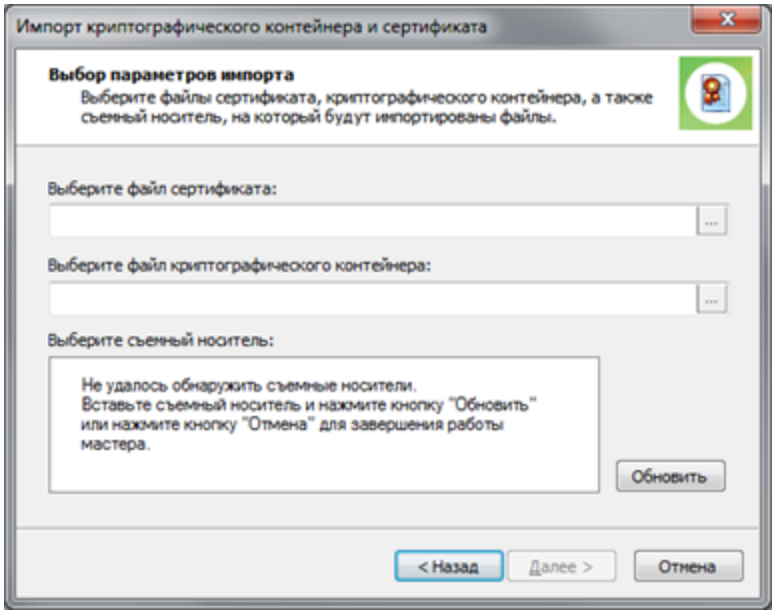
1. В основном окне программы нажмите кнопку "Импортировать...".

   На экране появится стартовый диалог программы-мастера.

   Совет. Если показывать этот диалог больше не требуется, отметьте поле "Не показывать ...".

2. Нажмите кнопку "Далее >".

   На экране появится диалог настройки параметров.



3. В текстовых полях диалога укажите пути к нужным файлам:
   - в поле "Выберите файл сертификата" — полный путь к файлу с расширением .cer, содержащему сертификат пользователя;
   - в поле "Выберите файл криптографического контейнера" — полный путь к файлу с расширением .p15 (или .p15_backup для резервной копии), содержащему закрытый ключ данного сертификата пользователя.

   Совет. Для выбора файла в диалоговом режиме нажмите кнопку "..." в правой части поля.

4. Вставьте USB-флеш-накопитель в свободный USB-разъем и нажмите кнопку "Обновить".
5. Выберите появившийся в нижнем поле диалога носитель и нажмите кнопку "Далее >".

   На экране появится диалог для ввода пароля.

   Примечание. Если для записи на носитель выбран только один из пары файлов и на указанном носителе нет пары для него, диалог для ввода пароля на экране не появится.

6. Введите пароль доступа к выбранному криптографическому контейнеру и нажмите кнопку "Далее >".

Будет выполнена проверка соответствия друг другу выбранных файлов сертификата и криптографического контейнера.

Если указан неверный пароль или криптографический контейнер не соответствует сертификату, на экране появится сообщение об этом.

Совет. Используйте кнопку "< Назад", чтобы вернуться к предыдущим диалогам и исправить допущенные ошибки.

При успешном завершении проверки начнется запись сертификата и криптографического контейнера на выбранный носитель. По окончании этой процедуры на экране появится диалог с перечнем выполненных действий.

7. Извлеките носитель из USB-разъема и нажмите кнопку "Готово".